NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Project 2014-02 Standard Drafting Team

February 19, 2014 | 9:00 a.m. – 5:00 p.m. ET
February 20, 2014 | 8:00 a.m. – 5:00 p.m. ET
February 21, 2014 | 8:00 a.m. – 12:00 p.m. ET

NERC
1325 G St. NW
Washington, DC 20005

Wednesday, February 19

1. **Welcome and Introductions***

   Participants were welcomed to the first in-person Project 2014-02 Standard Drafting Team meeting. Participants introduced themselves.

2. **NERC Antitrust Guidelines and Public Meeting Notice***

   The NERC Antitrust Guidelines and Public Meeting Notice were read.

3. **Determination of Quorum**

   The rule for a NERC Standard Drafting Team (SDT) states that a quorum requires two-thirds of the voting members of the SDT. There was a quorum with 10 out of 10 SDT members present.

4. **Expectations for SDT Members and Observers**

   There was a presentation on the expectations of SDT members and observers.

   a. Standards Development Process – Participant Conduct Policy*

      Participants reviewed the participant conduct policy.

   b. Email Listserv Policy*

      Participants reviewed the listserv policy.

5. **Overview of NERC Standard Processes Manual**

   NERC staff presented on the Standard Development process outlined in the Standard Processes Manual (SPM). There was a discussion on the plan to post the Reliability Standard Audit Worksheet (RSAW) concurrently with each posting of the standard. NERC staff noted that the RSAW will be posted within 15 days from the start of the standards' ballot and comment period and that this practice will be followed with other standards.

   NERC staff reviewed the latest revisions made to SPM regarding the response to comments obligations during the 45-day comment and ballot period. NERC staff noted that the SDT does not need to respond to every

comment but must respond to every issue raised in comments. The SDT may respond to comments in summary form.

6. **Summary of CIP V5 Revisions Technical Conference***

   NERC staff provided a brief summary of the technical conferences and noted that the summary is posted on the project page.

7. **Tentative Development Schedule**

   NERC staff displayed the proposed timeline for the milestones of the SDT that will be presented to the Standards Committee (SC). The SDT discussed dates for the next three in-person meetings and set a goal to post for the first comment and ballot period.

8. **Sub-Group Structure**

   a. Discuss approach and determine whether to use sub-groups.

      NERC staff and the SDT co-chairs introduced the sub-group concept. The face-to-face meetings would be focused on discussing the issues whereas the sub-groups would draft the language and focus on the four main directives issues. There was discussion that all SDT members and observers should participate in all sub-group activities as much as possible.

   b. Assign SDT members to four main directives sub-groups.

      The SDT was assigned to sub-groups as follows:

      IAC: Greg Goodrich and Scott Saunders; Low Impact: Jay Cribb and Forrest Krigbaum; Communication Networks: David Revill and David Dockery; and Transient Devices: Christine Hasha and Steve Brain.

   c. Schedule sub-group conference calls.

      The weekly call schedule was developed. For the schedule, please click here.

9. **Overview of Consideration of Issues and Directives Document**

   NERC staff introduced a document illustrating the FERC Order No. 791 directives, consideration of which will be important in NERC's filing when responding to the FERC directives. The document was used as a tool to discuss the scope of the SDT's work. NERC staff gave a status update of the VRFs/VSLs directives and the survey directive. Rule 320 of the NERC Rules of Procedure outlines the procedures for getting NERC Board of Trustees approval for revising VRFs and VSLs in response to a regulatory directive. The VRFs must be filed by May 5, 2014 and the VSLs must be filed by August 4, 2014.

10. **Discuss FERC Order No. 791 Directives for the SDT**

    a. Ensure common understanding of FERC directives and develop narrative for scoping.

       The meeting participants discussed the scope of work for each directive.

       Identify, Assess, and Correct (IAC) Directive:

       It was suggested that COM-002-4 has similar language to consider but some believe FERC may respond similarly to COM as it did to CIP. It was further noted that some of the IAC work is outside of the SDT's scope and within in the compliance realm. There was discussion about the removal of the IAC

language, in particular that language would have to be added to compensate for the IAC removal and make for a clear standard. The majority of meeting participants supported removal of the IAC language as a way to address the directive; however, participants noted their concerns including the lack of maturity of the Reliability Assurance Initiative (RAI) at present and that the underlying principles of the IAC language still be addressed. The SDT will engage in discussion with NERC compliance to coordinate on the issues.

Low Impact Assets Directive:

The SDT discussed some considerations for addressing the Low Impact assets directive, including the need to consider what sorts of assets are in the Low Impact category and what kinds of controls or criteria can be placed on those assets. There was a discussion on potential ways to group Low Impact assets, such as by generation or transmission, capacity factor, or raw megawatts. One participant noted that the Low Impact assets requirement in version 5 currently has IAC language in it. There was one suggestion that you can take some of the analogs that apply to Mediums and scale them to Lows.

Communication Networks Directive:

Participants noted that the SDT should consider what an entity can control and that some components may be under a vendor's control. Participants discussed the scope of the directive and noted that the one year timeframe is in relation to nonprogrammable components of communication networks. There was a suggestion that the SDT look to the history on this subject, particularly the FERC Order remanding an interpretation request on this topic and the history on physical ports. Participants noted that the SDT should be careful that whatever form the definition takes, it should comport with the rest of NERC standards.

Transient Devices Directive:

Participants noted that auditability would be a big issue in addressing this directive. Some examples were given of the types of controls and evidence, such as evidence can be a time log of when something came into Electronic Security Perimeter (ESP) or USB media policies and controls before a device enters. Participants stressed that the controls should be technology neutral, as technology is constantly changing. Participants noted the defense-in-depth strategy noted in the Order on P 134.

Thursday, February 20

11. **Identify, Assess, and Correct Language**

Meeting participants developed the following bullets as a scope of work for the IAC directive:

- Articulate the compliance concern that IAC addressed.
    - Identify audit/compliance issues associated with the removal of IAC.
        - Zero tolerance concerns
        - Self-correcting aspect
    - Discuss what the lines are between compliance and standards language. Consider examples from other standards.

- Consider alternatives to addressing clarifying the IAC language keeping with a move away from zero tolerance, but clarifying the compliance obligations.
- Determine whether to remove IAC language or utilize an alternative.
    - If IAC is removed, evaluate revisions to associated language such as measures and other language related to IAC.
    - Conduct outreach to vet IAC language or alternative.
    - Ensure RSAW is coordinated with revisions to requirements
- Evaluate what improves clarity and auditability and update requirement language for improved clarity and auditability.
- Coordinate with NERC compliance teams to address the concerns over removal of IAC, the zero tolerance, the implementation of a revised compliance approach (RAI) that impact stakeholder approval of the CIP revisions.
    - Include RAI individuals on sub-groups
    - Provide input on what RAI looks like for requirements
    - Ensure language and documents are revised from other departments

SDT members discussed how to get the trade associations' thoughts on removal of IAC and perhaps invite trade associations to a sub-group call.

Participants noted that the IAC sub-group needs participation from those involved with RAI, including standards, compliance, and enforcement. Participants said they would like to hear more from those involved with RAI in order to determine if it could fulfill the principles underlying the IAC language, such as moving away from zero defect requirements but maintaining self-correcting aspects of requirements. They further noted that the RSAW would play an important part in letting industry know compliance elements during standards development.

The SDT considered how to proceed if not removing IAC and whether there were alternatives. No one at the meeting presented an alternative at this time, but the SDT did not eliminate consideration of other approaches.

Acknowledging that work was needed regarding the compliance concerns raised, there was an informal straw poll as to whether participants were in favor of removing IAC as an approach to address the FERC directive. All ten SDT members, a large majority of in-room observers, and all but one participant on the web were in favor of removing IAC language from the standards.

Action items were then developed for the IAC sub-group to address at its calls and in between in-person meetings. The sub-group will consider the approach of removing the IAC language, but there has not been a final decision from the SDT at this time on an approach. The action items are in bullets below:

- Remove IAC from 17 requirements
    - What language and activities need to be revised per requirement?
        - Look to previous drafts
        - Avoid duplicating anything that may be covered in RAI
        - Consider P 81 criteria
    - Address self-correcting issues per requirement

        - Evaluate the use of action plans
        - Determine whether issues resolved by RAI
    - Change measures accordingly per requirement
    - What guidance does the SDT need to create per requirement?
        - Consider whether compliance language in measures needs to be addressed in guidance
    - Change VRF/VSLs accordingly
- Coordinate with compliance and enforcement
    - Ask NERC compliance to present on concepts in RAI to avoid duplication

12. **Communication Networks**

Meeting participants developed the following bullets as a scope of work for the Communication Networks directive:

- Develop new or modified standard
    - Determine whether to address communication networks in a new standard or through modification of existing standards and CIP and/or other family of standards
- Determine whether to develop a definition or other equally effective solution
    - If definition, define equipment and components to cover as communication networks.
        - Identify non-programmable equipment and components identified in the gap in P 150.
        - Draw from past communication network definition and requirement work
- Set a demarcation scope for covered communication networks keeping in mind entity control and auditing.
- Utilize the NIST SP 800-53 and ISO 27001 resources to inform scope, determination of risk and boundaries of communication networks.

Participants noted that the SDT will need to decide whether CIP standards may address the directive or if it needs to be under a different standards family.

There was a discussion as to what the Order meant by communication networks and what needs to be protected. Some participants noted that it should not go beyond the wires, cables, etc. as FERC mentioned communication mediums and the NIST 800-53 and ISO 27001 protections in its Order, implying that protections do not need to extend to hardware. Some noted that the FERC-led technical conference would provide more answers, but the SDT ultimately determined that it needed to move forward on the items specifically mentioned in the Order and deal with those issues if they arise at a later time.

FERC staff mentioned that NERC staff had filed a petition for an interpretation on CIP-006 in the past, and FERC had remanded the interpretation. FERC staff noted that the Order included some discussion on communication networks.

Meeting participants briefly discussed where to place these modifications, etc. in the standards, but no decisions were made.

Meeting participants then developed action items for the Communication Networks sub-group to address at its calls and in between in-person meetings. The action items are in bullets below:

1) Evaluate the gap in protection identified in Order

a. "Address security controls needed to protect the nonprogrammable components of communications networks" P 149
    i. Note P 143 on NOPR
    ii. Examples: "(i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays" P 149
    iii. Order remanding CIP-006 Interpretation
b. Identify nonprogrammable components
c. Delineate points/scoping

2) Identify protections that mitigate the Order-identified gap
3) Discuss modifying CIP-006 or other CIP standards

- Future Items
    - Definition?
    - Identify non-programmable equipment and components identified in the gap in P 150.
        - Develop controls based on equipment and components
        - Consider whether the requirement objectives inform the definition or does the definition inform the requirements
        - Should the definition for purposes of standard applicability be called something other than communication network?

13. **Low Impact Assets Protections**

Meeting participants developed the following bullets as a scope of work for the Low Impact assets directive:

- Consider how to make the requirements more auditable.
- Evaluate options to require specific controls, or develop objective criteria to evaluate adequacy of controls, or define processes with greater specificity for low impact facilities in order to address the ambiguity or an equally efficient solution.
- Consider whether subcategories of assets with defined control objectives would address the ambiguity, and if so, define the subcategories.
- Develop objective criteria to judge the sufficiency of protection for low impact assets.
- Keep in mind the low impact and low risk nature of these assets when revising requirements.
- Consider implications of the implementation schedule.
- Coordinate considerations with the revisions made to IAC language.

Meeting participants then developed action items for the Low Impact assets sub-group to address at its calls and in between in-person meetings. The action items are in bullets below:

- Focus on four technical areas in CIP-003-5 R2
- Evaluate and recommend options to address ambiguity described in P 108

- Options include require specific controls, or develop objective criteria to evaluate adequacy of controls, or define processes with greater specificity for low impact facilities in order to address the ambiguity or an equally efficient solution
- Consider other language related to requirement (i.e. Measures)

- Determine whether subcategories are appropriate
  - Could a site concept be leveraged in defining objective criteria?
- Consider documentation amount
- Determine whether taking out IAC makes Low Impact requirements need more language

14. **Transient Devices**

Meeting participants developed the following bullets as a scope of work for the Transient Devices directive:

- Identify the risks posed by transient devices. Where do the risks reside (the transient device, the BES Cyber Asset, BES Cyber System, BES)?
- Determine what qualifies as "adequately robust protection" against those risks.
- Identify the potential vulnerabilities presented by transient devices.
- Determine the characteristics that qualify a device as transient considering both what does and does not makes it a covered device (clarify inclusions and exclusions) (Is there a difference between "transient device" and "removable media"?)
- Consider the 6 security elements within P136 when designing the Reliability Standard and document the consideration.
  - (1) device authorization as it relates to users and locations;
  - (2) software authorization;
  - (3) security patch management;
  - (4) malware prevention;
  - (5) detection controls for unauthorized physical access to a transient device and;
  - (6) processes and procedures for connecting transient devices to systems at different security classification levels (i.e. High, Medium, Low Impact)
- Consider principles of defense-in-depth within the Reliability Standards

The SDT noted that the Version 5 drafting team had included some requirements for maintenance/transient devices in one of the previous postings. The SDT determined that the sub-group should look to the history in order to understand what issues had been discussed.

Meeting participants then developed action items for the Transient Devices sub-group to address at its calls and in between in-person meetings. The action items are in bullets below:

- Consider process
- Consider transient device classes
  - Consider levels of protection by device type
  - Consider requirements aimed toward device class

    - Consider whether protection should be from transient devices' risks
- Consider protecting BES
- Consider whether definition of transient devices is appropriate
    - Consider capability of device
- Consider checklist unless highly-managed device
- Consider the 6 security elements within Order 791 P 136 when designing the Reliability Standard and document the consideration.
    - (1) device authorization as it relates to users and locations;
        - Pre-authorization vs. scan each use
        - Consider procedural vs. technical controls
    - (2) software authorization; (applications on transient device)
        - Consider change management technical control
        - Consider configuration management
        - Consider NAC and High Impact
        - Consider whitelisting
        - Consider procedural vs. technical controls
    - (3) security patch management;
    - (4) malware prevention;
    - (5) detection controls for unauthorized physical access to a transient device and;
    - (6) processes and procedures for connecting transient devices to systems at different security classification levels (i.e. High, Medium, Low Impact)

Friday, February 21

15. **Standards Authorization Request Comments**

    Meeting participants discussed the SAR comments. NERC staff noted that some minor revisions would be made based on comments.

16. **Discuss and Prepare Project Plan for the NERC Standards Committee**

The SDT finalized the milestones in the proposed timeline. The timeline is as follows:

DRAFT Proposed Timeline for the Project 2014-02 Standard Drafting Team (SDT)		
Anticipated Date	**Location**	**Event**
1/15/2014	-	SC Authorizes SAR
1/29/2014	-	SC Appoints Standards Drafting Team
2/19/2014-2/21/2014	Washington, DC	SDT Meeting
3/18/2014-3/20/2014	Sacramento, CA	SDT Meeting
4/22/2014-4/24/2014	Atlanta, GA	SDT Meeting
5/12/2014-5/14/2014	Columbus, OH	SDT Meeting
6/2/2014	-	First 45-Day Comment Period & Ballot Opens
7/17/2014	-	First 45-Day Comment Period & Ballot Closes
8/29/2014	-	Second 45-Day Comment Period & Ballot Opens
10/13/2014	-	Second 45-Day Comment Period & Ballot Closes
10/31/2014	-	Final Ballot Opens
11/10/2014	-	Final Ballot Closes
11/13/2014	-	Presentation to NERC Board of Trustees for Adoption
12/31/2014	-	NERC Files Petition with the Applicable Governmental Authorities

17. **Action Items and Next Steps**

Sub-group calls would take place starting the first week of March. NERC staff would add the call times to the NERC calendar and distribute a calendar to the plus list. The schedule for the calls is here.

The SDT and NERC staff would work together to develop email and document management protocols for the sub-group calls.

There was a question about versioning of the standards, and the SDT noted that it would consider that issue during standards development.

There was a question on the implementation plan, and the SDT noted that it would work on it.

18. **Planning for Webinars, Full Team Calls, etc.**

    The SDT will hold weekly full team conference calls. The schedule for the calls is here.

19. **Discuss Industry Outreach Opportunities**

    a. Update Communications Plan.

    Participants looked at a list of upcoming outreach activities and industry events for the communications plan.

20. **Future Meeting Schedules and Venues**

    a. March 18-20, 2014 – Sacramento Municipal Utilities District - *Sacramento, CA*

    b. April 22-24, 2014 – NERC – *Atlanta, GA*

    c. May 12-14, 2014 – AEP - *Columbus, OH*

21. **Adjourn**